PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-317376
(43)Date of publication of application : 07.11.2003

(51)Int.Cl. G11B 20/10
G06F 12/14
G06F 15/00
H04N 7/173

(21)Application number : 2002-111555
(22)Date of filing : 15.04.2002

(71)Applicant : SONY CORP
(72)Inventor : KAWAMOTO HIROSHI
ISHIGURO RYUJI
EOMO YUICHI
NAGANO MOTOHIKO

(54) INFORMATION MANAGEMENT APPARATUS AND METHODRECORDING MEDIUMAND PROGRAM

(57)Abstract:
PROBLEM TO BE SOLVED: To prevent contents from being illegally utilized.
SOLUTION: Contents recorded on a CD 81 are captured by a ripping module 91 of a client 1 and saved in a storage part 28. In the client 1a contents ID (CID) for identifying contents and a unique ID (Uniq ID) intrinsic for the client 1 (ripping module 91) are generated and the IDs are added to the contents captured by the ripping module 91. Besidesin the client 1a right to use in which use conditions of contents or the like is described is generated and saved. In the right to use is described information representing that the reproduction of contents is permitted only in a device (client) having the same ID as the unique ID added to the contents. This invention can be applied to an information processor such as a personal computer.

CLAIMS

[Claim(s)]
[Claim 1]A contents acquisition means which acquires said contents in an information management device which manages contentsAn identification information acquisition means which acquires identification information which identifies said information

management deviceA content storing means which adds and memorizes said identification information acquired by said identification information acquisition means to said contents acquired by said contents acquisition meansAn information management device provided with a right-of-use memory measure which memorizes the right of use in which said identification informationsaid identification information added to said contentsand information to which use with the equipment with which the same identification information is acquired is permitted are included as information about use of said contents.

[Claim 2]The information management device according to claim 1 having further a reproduction means which reproduces said contents when said identification information added to said contents and said identification information acquired by said identification information acquisition means are the same.

[Claim 3]The information management device according to claim 1wherein said contents acquisition means acquires said contents from a predetermined recording medium with which said information management device was equipped.

[Claim 4]The information management device according to claim 1wherein said identification information acquisition means makes a generated random number said identification information.

[Claim 5]A contents acquisition step which acquires said contents in an information management method of an information management device which manages contentsAn identification information acquisition step which acquires identification information which identifies said information management deviceA contents memory step which adds and memorizes said identification information acquired by processing of said identification information acquisition step to said contents acquired by processing of said contents acquisition stepAn information management method containing a right-of-use memory step which memorizes the right of use in which information to which use with the equipment with which the identification information same as information about use of said contents as said identification information and said identification information added to said contents is set up is permitted is included.

[Claim 6]A contents acquisition control step which controls acquisition of said contents in a recording medium of an information management device which manages contentsAn identification information acquisition control step which controls acquisition of identification information which identifies said information management deviceA contents storage control step which controls memory performed to said contents acquired by processing of said contents acquisition control step by adding said identification information acquired by processing of said identification information acquisition control stepAs information about use of said contentssaid identification informationA recording medium with which a program which a computer containing a right-of-use storage control step which controls memory of the right of use in which information to which use with the equipment with which the same identification information as said identification information added to said contents is set up is

permitted is included can read is recorded.
[Claim 7]A contents acquisition control step which controls acquisition of said contents to a computer which controls an information management device which manages contentsAn identification information acquisition control step which controls acquisition of identification information which identifies said information management deviceA contents storage control step which controls memory performed to said contents acquired by processing of said contents acquisition control step by adding said identification information acquired by processing of said identification information acquisition control stepA program which performs a right-of-use storage control step which controls memory of the right of use in which information to which use with the equipment with which the identification information same as information about use of said contents as said identification information and said identification information added to said contents is set up is permitted is included.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention]This invention relates to the information management device which enables it to prevent unjust reproduction of contents easily especially and a methoda recording mediumand a program about an information management device and a methoda recording mediumand a program.
[0002]
[Description of the Prior Art]In recent yearsvarious kinds of broadband environment is being improved and the distribution service of various kinds of contentssuch as music data and a video datais beginning to be started completely.
[0003]For examplein [subscribed type (subscription type) music distribution service of "PressPlay (trademark)" etc. is performedand] this music distribution serviceWithin the limits of the conditions which a user is paying the charge of a monthly fixed amountand are set up beforehand. for examplethe case of streaming reproduction -- up to 1000 music -- refreshable and the case where download and it saves at the hard disk of a personal computer -- up to 100 music -- the preservation possibility of. When [to CD(Compact Disk)-R] writing in (copy)a music content can be used within the limits of which conditions that can be copied to 20 music.
[0004]By the wayfor example as a system which manages the right information data of the user who receives offer of the contents by such distribution service to JPH2001-352321A. In the system which arranges the node corresponding to two or more services to tree formFrom the node corresponding to predetermined service. Validation key blocks (EKB (Enabling Key Block)) including the key information (DNK (Device Node Key)) set as the node which exists on the path to the node (device) of

each leaf belonging to the service. Using is indicated.
[0005]In this systemEKB is added to the contents distributed in a certain serviceand the device which permits use of service is managed by making the updated key information which is included in EKB acquire using DNK given to each device. In this casethe device which cannot acquire the updated key information from EKB cannot receive offer of service after that using DNK.
[0006]And it enables it to manage use of the contents in each devicewithout this performing authenticating processing etc. each time between the server and device which provide contents.
[0007]In the system by which it does in this way and the right information data of contents are managedFor examplethe device which imported contents from CD (Compact Disk) is made as [manage / by ICV (Integrity Check Value) / the contents].
[0008]Drawing 1 is a figure showing the composition which manages the imported contents by ICV typically.
[0009]As shown in drawing 1for exampledevicessuch as a personal computerThe contents (music data) imported from CD are registered into the management table of a hard diskMAC (Message Authentication Code) (C1C2--Cn) generated based on the contents registered is applied to ICV=hash (KicvC1C2--Cn)and ICV is generated. Kicv is the key information for generating ICV.
[0010]And if it generates to a contents generate timeICV saved safely is compared with ICV newly generated to the predetermined timing at the time of reproductionetc. and the same ICV is obtainedIt is judged with there having been no alteration in contentsand when obtained ICV differs from the thing of a contents generate time on the other handit is judged with contents having had an alteration. After the case where it is judged with there having been no alteration in contentsregeneration of contents is performedand when judged with there having been an alterationregeneration is not performed. Thereforetherebyreproduction of the altered contents is prevented.
[0011]
[Problem to be solved by the invention]Howeverwhen managing contents by ICV as mentioned abovewhenever it imports contentsor whenever it reproduced contentsICV had to be generatedand SUBJECT that the processing burden was large occurred.
[0012]Thereforefor portable devicessuch as a device for music reproductionwhen the highly efficient operation part in which the hash operation for generating ICV is possible is needed and such operation part is providedthe cost of a device will go up as a result.
[0013]This invention is made in view of such a situationand enables it to prevent unjust reproduction of contents easily.
[0014]
[Means for solving problem]This invention is characterized by an information

management device comprising the following.
The contents acquisition means which acquires contents.
The identification information acquisition means which acquires the identification information which identifies an information management device.
The content storing means which adds and memorizes the identification information acquired by the identification information acquisition means to the contents acquired by the contents acquisition means.
The right-of-use memory measure which memorizes the right of use in which identification informationthe identification information added to contentsand the information to which use with the equipment with which the same identification information is acquired is permitted are included as information about use of contents.

[0015]The reproduction means which reproduces contents is established furtherand it may be made to reproduce contents only when the identification information by which the reproduction means is added to contentsand the identification information acquired by the identification information acquisition means are the same.
[0016]A contents acquisition means acquires contents from the predetermined recording medium with which the information management device was equipped.
[0017]It may be made to add an identification information acquisition means to contents etc. by making into identification information the random number which he generated. Identification information may be provided from external equipment etc.
[0018]This invention is characterized by the information management method of an information management device comprising the following.
The contents acquisition step which acquires contents.
The identification information acquisition step which acquires the identification information which identifies an information management device.
The contents memory step which adds and memorizes the identification information acquired by processing of the identification information acquisition step to the contents acquired by processing of the contents acquisition step.
The right-of-use memory step which memorizes the right of use in which the information to which use with the equipment with which the identification information same as information about use of contents as identification information and the identification information added to contents is set up is permitted is included.

[0019]The contents acquisition control step which controls acquisition of contents in the recording medium of the information management device of this inventionThe identification information acquisition control step which controls acquisition of the identification information which identifies an information management deviceThe contents storage control step which controls the memory performed to the contents acquired by processing of the contents acquisition control step by adding the identification information acquired by processing of the identification information

acquisition control stepThe right-of-use storage control step which controls memory of the right of use in which the information to which use with the equipment with which the identification information same as information about use of contents as identification information and the identification information added to contents is set up is permitted is includedThe program which a computer is made to execute is recorded.

[0020]The contents acquisition control step which controls acquisition of contents to the computer by which the program of this invention controls the information management device which manages contentsThe identification information acquisition control step which controls acquisition of the identification information which identifies an information management deviceThe contents storage control step which controls the memory performed to the contents acquired by processing of the contents acquisition control step by adding the identification information acquired by processing of the identification information acquisition control stepThe right-of-use storage control step which controls memory of the right-of-use information in which the information to which use with the equipment with which the identification information same as information about use of contents as identification information and the identification information added to contents is set up is permitted is included is performed.

[0021]In the information management device of this inventiona methodand a programcontents are acquired and the identification information which identifies an information management device is acquired. The acquired identification information is added and memorized to the acquired contentsand as information about use of contentsThe right of use in which identification informationthe identification information added to contentsand the information to which use with the equipment with which the same identification information is acquired is permitted are included is memorized.

[0022]

[Mode for carrying out the invention]Drawing 2 shows the composition of the contents providing system which applied this invention. Client 1-11-2 (hereafterwhen these clients do not need to be distinguished separatelythe client 1 is only called) is connected to the Internet 2. In this examplealthough two clients are shownthe client of the arbitrary number is connected to the Internet 2.

[0023]On the Internet 2. When the content server 3 which provides contents to the client 1the license server 4 which gives the right of use required to use the contents which the content server 3 provides to the client 1and the client 1 receive the right of useThe fee collection server 5 which performs accounting to the client 1 is connected.

[0024]Only the number also with arbitrary these content servers 3license server 4and fee collection server 5 is connected to the Internet 2.

[0025]Drawing 3 expresses the composition of the client 1.

[0026]In drawing 3CPU(Central Processing Unit) 21Various kinds of processings are performed according to the program memorized by ROM(Read Only Memory) 22 or the program loaded to RAM(Random Access Memory) 23 from the storage parts store 28. the timer 20 -- a time check -- it operates and time information is supplied to CPU21. To RAM23CPU21 performs various kinds of processings againand also required data etc. are memorized suitably.
[0027]The encryption decoding part 24 performs processing which decodes the already enciphered contents while enciphering contents. For examplethe codec part 25 encodes contents by ATRAC(Adaptive Transform Acoustic Coding)3 system etc.and is made to supply and record them on the semiconductor memory 44 connected to the drive 30 via the input/output interface 32. Or the codec part 25 decodes the data which was read from the semiconductor memory 44 via the drive 30 and which is encoded again. The semiconductor memory 44 is constituted by the memory stick (trademark) etc.for example.
[0028]CPU21ROM22RAM23the encryption decoding part 24and the codec part 25 are mutually connected via the bus 31. The input/output interface 32 is also connected to this bus 31 again.
[0029]The input part 26CRT (Cathode Ray Tube) which become the input/output interface 32 from a keyboarda mouseetc.The communications department 29 which comprises the storage parts store 28a modema terminal adopteretc. which comprise the outputting part 27 which consists of a display which consists of LCD (Liquid Crystal Display) etc.a loudspeakeretc.a hard disketc. is connected. The communications department 29 performs the communications processing through the Internet 2. The communications department 29 performs the communications processing of an analog signal or a digital signal among other clients again.
[0030]The drive 30 is connected to the input/output interface 32 again if neededIt is suitably equipped with the magnetic disk 41the optical disc 42the magneto-optical disc 43or the semiconductor memory 44and the computer program read from them is installed in the storage parts store 28 if needed.
[0031]Although a graphic display is omittedthe content server 3the license server 4and the fee collection server 5 are also constituted by the client 1 shown in drawing 3and the computer which has the same composition fundamentally. Thenin the following explanationthe composition of drawing 3 is quoted also as composition of the content server 3the license server 4the fee collection server 5etc.
[0032]In this inventionas shown in drawing 4a device and a key are managed based on the principle of a broadcasting yne KURIPUSHON (Broadcast Encryption) system. A key is made into a class tree structure and is equivalent to a key with leaf (leaf) of the bottom peculiar to each device. The class tree structure lock management used for the system of this invention is indicated to JP2001-352321A. In the case of the example of drawing 4the key corresponding to 16 devices from the number 0 to the number 15 is generated.

[0033]Each key is specified corresponding to each node of the tree structure shown by a figure Nakamaru seal. Corresponding to the root node of the highest rungthe route key KR (it is also suitably called Kroot) is prescribed by this exampleand the key K0 and K1 are prescribed corresponding to the 2nd step of node. Corresponding to the 3rd step of nodethe keys K00 thru/or K11 are specifiedand the key K000 thru/or the key K111 are specified corresponding to the node of the 4th step. And the keys K0000 thru/or K1111 support the leaf (device node) as a node of the bottomrespectively.
[0034]Since it is considered as the layered structurethe key of the higher rank of the key K0010 and the key K0011 is set to K001and the key of the higher rank of the key K000 and the key K001 is set to K00for example. Hereaftersimilarlythe key of the higher rank of the key K00 and the key K01 is set to K0and the key of the higher rank of the key K0 and the key K1 is set to KR.
[0035]The key using contents is managed by the key corresponding to each node of one path from the device node (leaf) of the bottom to the root node of the highest rung. For examplein the device corresponding to the leaf of the number 3the key for using contents is managed by each key of the path containing the key K0011K001K00K0and KR.
[0036]In the system of this inventionas shown in drawing 5it is a keying system constituted based on the principle of drawing 4and management of the key of a device and the key of contents is performed. In the example of drawing 58+24+32 steps of nodes are made into a tree structureand a category corresponds to each node from a root node to eight steps of a low rank. The category in here means categoriessuch as a category of the apparatus which uses semiconductor memorysuch as a memory stickfor exampleor a category of apparatus which receives digital broadcasting. And this system (T system is called suitably) corresponds to one node in this category node as a system which manages the right of use.
[0037]That isthe service which a service provider or a service provider provides corresponds by the key corresponding to 24 steps of a younger class's nodes further from the node of T system. Thereforein the example of drawing 5the service provider of 2^{24} (about 16 mega) or service can be specified. 32 steps of classes of the bottom can prescribe the user (client 1) of 2^{32} (about 4 giga). The key corresponding to each node on the path from 32 steps of nodes of the bottom to the node of T system constitutes DNK (Device Node Key)and ID corresponding to the leaf of the bottom is set to leaf ID.
[0038]The contents key which enciphered contents is enciphered by updated route key KR'and the updating node key of the class of a higher rankIt is enciphered using the updating node key of the class of the latest low rankand is arranged in EKB (Enabling Key Block: validation key blocks) (with reference to drawing 7it mentions later).
[0039]The updating node key of the stage on one is enciphered from the end in EKB

by the node key or leaf key of an end of EKBand it is arranged in EKB. One key of the DNK(s) described by service information is used for the client 1Using the node key which decoded the updating node key of the class of the latest higher rank described by EKB distributedand decoded and obtained it with contentsit is described by EKB and also the updating node key of the class on it is decoded. By performing same processing one by onethe client 1 can obtain updating route key KR'. Service information is supplied from the license server 4when the information about the client 1 is registeredand it calls a license the combination of the right of use which are this service information and the information which are mentioned laterand to which use of specific contents is permitted.

[0040]Drawing 6 is a figure showing the concrete example of a classification of the category of a class tree structure.

[0041]In drawing 6route key KR2301 is set to the highest rung of a class tree structurethe node key 2302 is set to the following intermediate stagesand the leaf key 2303 is set to the bottom. Each device holds the device node key (DNK) which consists of each leaf keyand a series of node keys from a leaf key to a route key and a route key.

[0042]The predetermined node of the Mth step (the example of drawing 5 M= 8) is set up as the category node 2304 from the highest rung. That islet each of the node of the Mth step be a device setting-out node of a specific category. Let M+1 or less step of nodeand a leaf be the node and leaf about the device contained in the category by making one node of the Mth step into the peak.

[0043]For examplea category [memory stick (trademark)] is set to the one node 2305 of the Mth step of drawing 6and a node which stands in a row below in this nodeand a leaf are set up as a node or a leaf only for a category containing various devices which use memo RISUTEIIKU. That is2305 or less node is defined as a related node of a device defined as a category of a memory stickand a set of a leaf.

[0044]A low-ranking stage can be set up as the subcategory node 2306 by several steps from M stage. In an example of drawing 6the node 2306 of [a vessel only for reproduction] is set up as a subcategory node contained in a category of a device which uses a memory stick for a node under two steps of the category [memory stick] node 2305. To 2306 or less node of a vessel only for reproduction which is a subcategory node. The node 2307 of a telephone with a music reproduction function included in a category of a vessel only for playback is set upand the [PHS] node 2308 contained in the low rank at a category of a telephone with a music reproduction function and the [cellular-phone] node 2309 are set up further.

[0045]A category and a subcategory only not only in the kind of devicefor example A certain makerIt is possible to set up in arbitrary units (these are generically called an entity hereafter)such as the node which a content providera settlement-of-accounts organizationetc. manage uniquelyi.e.a batcha jurisdiction unitor a providing service unit.

[0046]For exampleby setting up one category node as a peak node only for game

machine machine XYZ which a game machine machine maker sellsIn the game machine machine XYZ which a maker sellsthe node key of the lower berth below the peak nodeBy being able to store and sell a leaf keyand generating and distributing after that EKB constituted by the node key below the peak node keyand the leaf key. The message distribution processing of enciphered contentthe message distribution processing of various keysan update processetc. can be performed only to the device (game machine machine XYZ) below a peak node.

[0047]That isrenewal of a keyetc. can be performedwithout completely affecting the device belonging to the node of other categories which is not classified as a peak node.

[0048]When it is revealed in t at a certain time that the key K0011 which the device 3 ownsK001K00K0and KR were analyzed by the aggressor (hacker)and it was exposed of KRAfter itin order to protect the data transmitted and received by a system (group of the devices 012and 3)it is necessary to separate the device 3 from a system. for that purpose -- a node key -- K -- 001 -- K -- 00 -- K -- zero -- KR -- respectively -- being new -- a key -- K -- (-- t --) -- 001 -- K -- (-- t --) -- 00 -- K -- (-- t --) -- zero -- K -- (-- t --) -- R -- updating -- a device -- zero -- one -- two -- the -- updating -- a key -- it is necessary to tell . Hereit is shown that K(t) aaa is an updating key of the generation (Generation) t of the key Kaaa.

[0049]distribution **** of an updating key -- it ****** just. Renewal of a key is performed by storing in a predetermined recording medium the table constituted by EKB shown in drawing 7for exampleand supplying it to the devices 01and 2 via a network. EKB is constituted by the cryptographic key for distributing the key newly updated by the device corresponding to each leaf (node of the bottom) which constitutes a tree structure as shown in drawing 4.

[0050]EKB shown in drawing 7 is constituted as block data with the data configuration which can update only the required device of renewal of a node key. In the devices 01and 2 in the tree structure shown in drawing 4the example of drawing 7 is the block data formed for the purpose of distributing the generation's t updating node key.

[0051]The devices 0 and 1 are received so that clearly from drawing 4updating -- a node key -- ****** -- K -- (-- t --) -- 00 -- K -- (-- t --) -- zero -- K -- (-- t --) -- R -- providing -- things -- required -- a device -- two -- receiving -- updating -- a node key -- ****** -- K -- (-- t --) -- 001 -- K -- (-- t --) -- 00 -- K -- (-- t --) -- zero -- K -- (-- t --) -- R -- providing -- things -- being required .

[0052]As shown in EKB of drawing 7two or more cryptographic keys are contained in EKBfor examplea cryptographic key of the bottom of drawing 7 is Enc (K0010K(t)001). this -- a device -- two -- having -- a leaf key -- K -- 0010 -- enciphering -- having had -- updating -- a node key -- K -- (-- t --) -- 001 -- it is -- a device -- two -- oneself -- having -- a leaf key -- K -- 0010 -- a cryptographic key -- decoding -- updating -- a node key -- K -- (-- t --) -- 001 -- being acquirable .

[0053]using updating node key K(t)001 obtained by decodingthe device 2 can decode the 2nd step of cryptographic key Enc (K -- (-- t --) -- 001 -- K -- (-- t --) -- 00) from under drawing 7and can acquire updating node key K(t)00.
[0054]The device 2 is decoding the 2nd step of cryptographic key Enc (K (t) 00K(t)0) from on drawing 7 similarlyUpdating node key K (t) 0 can be acquired and updating route key K(t) R can be acquired from on drawing 7 using this by decoding the 1st step of cryptographic key Enc (K(t) 0 and K (t) R).
[0055]on the other hand -- a node key -- K -- 000 -- updating -- an object -- a key -- containing -- not having -- a node -- zero -- one -- updating -- a node key -- ****** -- being required -- a thing -- K -- (-- t --) -- 00 -- K -- (-- t --) -- zero -- K -- (-- t --) -- R -- it is .
[0056]The nodes 0 and 1 acquire updating node key K(t)00 using the debye skiing K0000 and K0001 by decoding the 3rd step of cryptographic key Enc (K000K(t)00) from on drawing 7Similarly one by one by decoding the 2nd step of cryptographic key Enc (K (t) 00K(t)0) from on drawing 7. Updating node key K (t) 0 is acquired and updating route key K(t) R is further acquired from on drawing 7 by decoding the 1st step of cryptographic key Enc (K(t) 0 and K (t) R). Thusthe devices 01and 2 can obtain updated key K(t) R.
[0057]The index of drawing 7 shows the actual address of the node key and leaf key which are used as a decryption key for decoding the cryptographic key shown in the right-hand side of a figure.
[0058]When renewal of node key K(t) 0 and K (t) R of the upper stage of the tree structure shown in drawing 4 is unnecessary and the update process of only the node key K00 is requiredupdating node key K(t)00 can be distributed to the devices 01and 2 by using EKB of drawing 8.
[0059]EKB shown in drawing 8 is available when distributing the new contents key shared in a specific groupfor example.
[0060]For examplethe devices 012and 3 in the group to whom it is shown with the alternate long and short dash line of drawing 4 use a certain recording mediumand presuppose that it is required to set up new common contents key K(t) con to those devices. this -- the time -- a device -- zero -- one -- two -- three -- being common -- a node key -- K -- 00 -- having updated -- K -- (-- t --) -- 00 -- being new -- being common -- updating -- a contents key -- K -- (-- t --) -- con -- enciphering -- having had -- data -- Enc (K (t) 00K(t) con) -- drawing 8 -- being shown -- having -- EKB -- distributing -- having . By this distributionthe distribution as data of the device 4 etc. which other groups' apparatus cannot decode is attained.
[0061]That isthe devices 01and 2 can obtain contents key K(t) con at the t time by decoding code data using key K(t)00 which processed and obtained EKB.
[0062]Drawing 9 as an example of processing which obtains contents key K(t) con in t timeK (t) The data Enc (K (t) 00K(t) con) in which new common contents key K(t) con was enciphered by 00and EKB shown in drawing 8 are the figures showing typically

processing of the device 0 provided via a predetermined recording medium. That isan example of drawing 9 is an example which set encryption message data based on EKB to contents key K(t) con.
[0063]As shown in drawing 9the device 0 generates node key K(t)00 using EKB at the generation t time stored in a recording mediumand the node key K000 currently beforehand prepared for itself by EKB processing (processing which undoes a key one by one) which was mentioned above. In order to decode updating contents key K(t) con and to use it behind using updating node key K(t)00 decodedthe device 0 is the leaf key K0000 which he hasand enciphers and stores updating contents key K(t) con.
[0064]Drawing 10 is a figure showing the example of a format of EKBand EKB which consists of such various kinds of information is contained in the header of contents data.
[0065]The version 61 is an identifier which shows the version of EKB. This version 61 has the function to identify the newest EKBand a function which shows a correspondence relation with contents. The depth 62 shows the hierarchy number of the class tree to the device of the distribution destination of EKB. The data pointer 63 is a pointer in which the position of the data division 66 in EKB is shownand the tag pointer 64 and the signature pointer 65 are pointers in which the position of the tag part 67 and the signature 68 is shownrespectively.
[0066]The data produced byfor examplethe node key to update being enciphered is stored in the data division 66. For exampleeach cryptographic key about the updated node key as shown in drawing 9 is stored in the data division 66.
[0067]The tag part 67 is a tag which was stored in the data division 66 and in which the physical relationship of the node key and leaf key which were enciphered is shown. The grant rule of this tag is explained with reference to drawing 11.
[0068]In the example of drawing 11as shown in drawing 11 Blet the data sent be a cryptographic key of drawing 7. Let the address of the top node contained in a cryptographic key be a top node address.
[0069]In this examplesince updating key K(t) R of a route key is containeda top node address serves as KR. At this timethe data Enc (K(t) 0 and K (t) R) of the highest rung corresponds to the position P0 shown in a class tree shown in drawing 11 Afor example. Data of the following stage is Enc (K (t) 00K(t)0)and corresponds to the position P00 at the lower left of the front data Enc (K(t) 0 and K (t) R) on a tree.
[0070]That iswhen it sees from a position of a tree structure and data is in the bottom of ita tag is set as 0and when there is no dataa tag is set as 1. A tag is set up as [a left (L) tag and a right (R) tag].
[0071]Since it is set to L tag =0 since there is data in the position P00 at the lower left of the position P0 corresponding to the data Enc (K(t) 0 and K (t) R) of the highest rung of drawing 11 Band there is no data in the lower right of the position P0it is set to R tag =1. Hereaftera tag is set as all the data and a data row shown in drawing 11 C and a tag sequence are constituted.

[0072]A tag is set up in order that the corresponding data Enc (KxxxKyyy) may show where [of a tree structure] it is located. the key data Enc (KxxxKyyy) stored in the data division 66 -- although ... is only enumeration data of the key enciphered simplydistinction of the position on the tree of the cryptographic key stored as data of it is attained with the tag mentioned above. Without using a tagas shown in drawing 7 or drawing 8the node index to which encryption data was made to correspond is usedfor example0:Enc(K(t) 0 and K (t) R)00:Enc(K -- (-- t --) -- 00 -- K -- (-- t --) -- 0)000:Enc (K ((-- t --) -- 000 -- K -- (-- t --) -- 00)although it is also possible to consider it as a data configuration like ...) When it has composition using such an indexin the distribution etc. which the data volume increases and pass a networkit is not desirable. On the other handdistinction of the position of a key is attained with smaller data volume by using the above tags as index data in which the position of a key is shown.

[0073]Returning to explanation of drawing 10the signature (Signature) 68 is an electronic signature which published EKBfor examplea lock management center (license server 4)contents ROBAIDA (content server 3)a settlement-of-accounts organization (fee collection server 5)etc. perform. The device which received EKB judges whether acquired EKB is EKB which the just publisher published by verifying the signature included in EKB.

[0074]Drawing 12 is a figure in which the contents currently recorded on CD81 show typically the processing incorporated by the client 1 in the above key management systems.

[0075]CPU21 of the client 1 controls the ripping module 91 which comprises executing a predetermined programand makes the contents memorized by CD81 connected to the client 1 incorporate.

[0076]CPU21 makes the storage parts store 28 memorize data obtained by adding content ID (CID) and ID (unique ID (Uniq ID)) set up as a peculiar thing to the client 1 to contents incorporated with the ripping module 91. This unique ID is a random number which consists of a predetermined digit numberfor exampleand the same unique ID as what was added to contents is saved by the client 1.

[0077]CPU21 generates the right of use of contents incorporated with the ripping module 91 as service in a key management system mentioned above. For examplewhen contents from which the ripping module 91 was incorporated by that cause are the modules whose check-out is enabled only 3 timesthe right of use a service condition showing the ability to check out only 3 times was described to be is generated. Content ID and unique ID which were added to contents are also described by the right of useand matching of contents and the right of use is made.

[0078]In a client reproduced when reproducing contents incorporated as mentioned aboveIt is not only judged whether reproduction is permitted by the right of usebut it is judged whether unique ID added to contents and unique ID of a client which reproduces the contents are the same. And regeneration of contents is performed

only when unique ID which reproduction of contents is permitted by the right of useand is added to contentsand unique ID of a client which generates contents are the same. That isin a client which acquired only contents and the right of use by a copy etc.temporarilyeven if it is a case where reproduction is permitted by the right of usethe contents can be reproduced.

[0079]Hereaftercontents are incorporated and a series of processings of the client 1 using it are explained with reference to a flow chart.

[0080]Processing of the client 1 which incorporates contents is explained with reference to the flow chart of introduction and drawing 13.

[0081]For examplewhen it is directed that the drive 30 of the client 1 is equipped with predetermined recording mediasuch as CD81 (optical disc 42) on which contents were recordedand contents are incorporatedCPU21 of the client 1 controls the ripping module 91 which comprises executing a predetermined programand incorporates contents in Step S1.

[0082]CPU21 generates the content ID which identifies contents in Step S2. In Step S3CPU21 to the client 1 (ripping module 91) peculiar unique IDFor examplewhen it judges whether the storage parts store 28 memorizes and judges with it not being memorizedit progresses to step S4 and unique ID which consists of a predetermined digit number is generated. Generated unique ID is saved at the storage parts store 28.

[0083]It is not what was generated in the client 1 as unique IDFor examplewhen the user of the client 1 registers predetermined information into the license server 4 so that he may make the ripping module 91 availableit may be made to use what is given to the client 1 from the license server 4. Thuswhen unique ID is givenor when already being generated in ripping performed in the pastin Step S3 of drawing 13it is judged with there being unique ID and processing of step S4 is skipped.

[0084]CPU21 is described in Step S5 to "Attribute (attribute)" as a field where the predetermined attribution information of contents is described in content ID and unique ID. The format of contents is explained in full detail behind.

[0085]In Step S6CPU21 creates the digital signature based on the information described as attribution information using its own secret key. This secret key is provided from the license server 4for examplewhen the information about the client 1 is registered.

[0086]In Step S7CPU21 creates data of a header recorded corresponding to contents. Data of a header is constituted by URL showing an access point for acquiring content IDright-of-use IDand the right of useand watermark.

[0087]CPU21 creates a digital signature based on data of a header created by processing of Step S7 in Step S8 using its own secret key. CPU21 makes contents encipher in step S9 by a contents key which controlled and generated the encryption decoding part 24. Informationincluding generated contentsa header which accompanies itetc.is saved in Step S10 at the storage parts store 28.

[0088]Drawing 14 is a figure showing an example of a format of contents.

[0089]Data (Enc (KrootKc)) produced by contents enciphering a headerEKBand the contents key Kc by the route key Kroot as shown in drawing 14Attribution information content ID and unique ID are described to be (Attribute)A certificate (Cert)a digital signature generated based on a header (Sig (Header))It comprises data (Enc (KcContent))the metadata (Meta Data)and the mark (Mark) which are produced by enciphering contents by the contents key Kc.
[0090]Content ID (CID)right-of-use ID (right-of-use ID) which identifies the right of use corresponding to contentsURL showing the acquisition place (client 1) of the right of useand a watermark (WM) are described by the header.
[0091]Artist ID as identification information for identifying record company ID as identification information for identifying the donor of content ID and contents and an artistunique IDetc. are contained in the attribute of contents. In this examplesince the contents which are the targets of the right of use are specifiedan attribute is used.
[0092]Metadata is various kinds of information relevant to contentsfor examplethe data of a jacketa photographwordsetc. is added to contents as metadata to a music content. The digital signature generated based on a user's ID (leaf ID)an ownership flagbeginning-of-using timecopy frequencyand these information is described by the mark. The ownership flag of a mark is added when only a predetermined periodfor examplebuys the right of use which makes contents usable as it was (when duration of service is changed into a using [it]-eternally thing). Histories (log)such as the number of times which copied the contentsare described by the copy frequency of a mark.
[0093]Although the case where contents were acquired from CD81 above (ripping) was explainedFor exampleabout the contents acquired from the predetermined server via the Internet 2similarlyunique ID of the client 1 is added with content IDand it is saved by the client 1.
[0094]Nextwith reference to the flow chart of drawing 15processing of the client 1 which generates the right of use corresponding to the incorporated contents is explained.
[0095]In Step S21the right of use beforehand set up as what is given to the contents incorporated with the ripping module 91 is read from the storage parts store 28 as the right of use corresponding to the contents incorporated by processing of drawing 13. Informationincluding right-of-use IDa versionthe date and time of creationthe term of validityetc.is described by the right of use memorized by the storage parts store 28.
[0096]In Step S22only in the client 1 to which the same ID as unique ID described as attribution information of contents is setCPU21 adds the information showing the contents being renewable while adding unique ID to the selected right of use. In Step S23CPU21 chooses a service condition and adds it. For examplewhen it is set up that the contents incorporated by that cause can check out only 3 times simultaneously to the ripping module 91the service condition showing the ability to check out only 3 times is chosen. When it is set up that the contents incorporated by that cause can

copy freely to the ripping module 91 for examplethe service condition showing it is chosen.
[0097]In Step S24CPU21 creates the digital signature of the data described by the right of use selected as mentioned aboveand adds it. The right of use to which the digital signature was added is saved in Step S25 at the storage parts store 28.
[0098]Drawing 16 is a figure showing the example of a format of the right of use.
[0099]A version is information which divides a major version and a minor version by a dotand describes the version of the right of use. A profile is information which is described from the integral value of a decimal and specifies the restriction to the describing method of the right of use. Right-of-use ID is identification information for identifying the right of use described by a hexadecimal constant. The date and time of creation shows the date on which the right of use was created. The term of validity shows the term of validity of the right of use. It is shown that the term of validity which is 59 minutes and 59 seconds will not have restriction in the term of validity at 23:00 in 9999. The expiration date which can use contents for a service condition based on the right of useThe reproduction term which can reproduce contents based on the right of useThe number of times which can copy contents based on the maximum reproduction frequency of contentsand its right of use (copy frequency allowed)The information which shows the number of times which can be copied [whether contents are recordable on CD-R and] to PD (Portable Device) based on the number of times of the maximum check-out and its right of usethe propriety of movement of the right of usethe existence of duty to take a use logetc. is included. The electronic signature of a service condition is an electronic signature corresponding to a service condition.
[0100]A constant is a constant referred to by the service condition or a busy condition. Unique ID is generated when incorporating contents. An electronic signature is an electronic signature corresponding to the whole right of use. A certificate is a certificate containing the public key of the license server 4.
[0101]In accordance with a service condition of the right of usea busy condition (contents conditions) which is the information showing a state of contents or the right of use is memorized by the storage parts store 28 of the client 1. The number of times which reproduced contents based on the right of use corresponding to a busy conditionInformation which shows hysteresis information about the number of times which copied contentsthe number of times which checked out contentsthe first time to reproduce contentsthe number of times which recorded contents on CD-Rother contentsor the right of useetc. is included. A judgment of conditions of reproduction of contents is performed based on a service condition included in the right of useand a busy condition memorized by the storage parts store 28 with the right of use. For examplewhen there is less number of times which reproduced contents memorized by busy condition than the contents maximum reproduction frequency contained in a service conditionit is judged with reproductive conditions being fulfilled.

[0102]Nextwith reference to a flow chart of drawing 17regeneration of contents by the client 1 which incorporated contents with the ripping module 91 is explained.
[0103]In Step S41CPU21 of the client 1 reads unique ID described as attribution information of the contents which read and read the contents to which it pointed because a user operates the input part 26 from the storage parts store 28 based on content ID. CPU21 reads unique ID which reads the right of use corresponding to the contents reproduction was instructed to be based on right-of-use IDand is described by the read right of use in Step S42.
[0104]Unique ID which CPU21 saved in Step S43Namelyunique ID of the client 1 is read from the storage parts store 28It progresses to Step S44 and it is judged whether all of unique ID described by those unique IDi.e.unique ID described by contentsand the right of use and unique ID saved at the client 1 are the same. It may be made to be judged whether only unique ID described by contents and unique ID saved at the client 1 are the same.
[0105]When it judges with all the unique ID of CPU21 being the same in Step S44it progresses to Step S45 and it is judged by the right of use whether use of contents is permitted based on the service condition described. For exampleCPU21 judges whether the term of validity (refer to drawing 16) as a descriptive content of the right of use and use of whether the right of use is a thing within the term of validity by comparing the present date clocked by the timer 20 and contents are permitted.
[0106]In Step S45when judged with use being permitted by the right of useit progresses to Step S46 and CPU21 performs processing which decodes the contents (read) memorized by RAM23. The contents decoding processing performed in Step S46 is later mentioned with reference to the flow chart of drawing 18.
[0107]CPU21 supplies the contents decoded by the encryption decoding part 24 to the codec part 25and makes them decode in Step S47. And CPU21 supplies and carries out digital to analog conversion of the data decoded by the codec part 25 to the outputting part 27 via the input/output interface 32and is made to output from a loudspeaker.
[0108]Unique ID described by contents at Step S44When judged with unique ID (unique ID further described by the right of use) saved at the client 1 differingat Step S45. When judged with reproduction of contents not being permitted by the right of usein Step S48error handling is performed and processing is ended after that.
[0109]Nextwith reference to the flow chart of drawing 18the details of the decoding processing of the client performed in Step S46 of drawing 17 are explained.
[0110]In Step S61by DNK which was contained in service information and provided from the license server 4CPU21 of the client 1 decodes the key information included in EKB one by oneand acquires the route key Kroot (KR). It progresses to Step S62 and CPU21 decodes the contents key Kc using the route key Krootwhen the route key Kroot is acquired. As shown in drawing 14the data Enc (KrootKc) produced by the contents key Kc being enciphered by the route key Kroot is added to contents.

[0111]In Step S63CPU21 decodes contents by the contents key Kc acquired at Step S62.
[0112]Drawing 19 expresses the above decoding processing typically. In drawing 19contents are saved by the client 1 and only the main information is shown among the information shown in drawing 14.
[0113]By namelythe route key Kroot which the route key Kroot was acquired (Step S61 of drawing 18)and was acquired from EKB based on DNK with which the client 1 was provided from the license server 4. The data Enc (KrootKc) is decoded andtherebythe contents key Kc is acquired (Step S62 of drawing 18). And the data Enc (KcContent) is decoded by the contents key Kcand the contents (Content) are acquired (Step S63 of drawing 18). As shown in drawing 20the data Enc (DNKKroot) produced by the route key Kroot being enciphered by DNK is contained in EKB of drawing 14 and drawing 19.
[0114]Contents can be reproduced even if it is the client (client by which unique ID is not managed) which acquired the right of use unjustly with contents by controlling reproduction of contents as mentioned above.
[0115]When it is carried out that the contents incorporated by the client 1 by the above processing can check out (when it is set up as a service condition that he can check out)To other clients which receive check-out of contents from the client 1it is enciphered by a predetermined method and contentsthe right of useand unique ID of the client 1 may be made to provide. In that casein the client which received offer of those informationthe same processing as what is shown in drawing 17 and drawing 18 is performedand reproduction of contents is performed. Therebycheck-out/check-in of the contents under management of the client 1 from which contents were incorporated first are performed.
[0116]In the above-mentioned embodimentsince the right of use required in order to use contents was specifiedcontents conditions of the attribute of contents and the right of use were usedbut it does not restrict to this. For examplesince it is decided that the right of use required if it may be made for right-of-use ID of the right of use required in order to use these contents to be included in contents and contents are specified as them in this casein order to use it will be a meaningit does not need to perform processing which determines both matching.
[0117]
[Effect of the Invention]According to this inventioncontents can be provided.
[0118]According to this inventionuse of inaccurate contents can be prevented.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1]It is a mimetic diagram of the managerial system of the conventional

contents.
[Drawing 2]It is a figure showing the example of composition of the contents providing system which applied this invention.
[Drawing 3]It is a block diagram showing the example of composition of the client of drawing 2.
[Drawing 4]It is a figure showing the composition of a key.
[Drawing 5]It is a figure showing a category node.
[Drawing 6]It is a figure showing the example of correspondence of a node and a device.
[Drawing 7]It is a figure showing the example of composition of validation key blocks.
[Drawing 8]It is a figure showing other examples of composition of validation key blocks.
[Drawing 9]It is the figure which expressed use of validation key blocks typically.
[Drawing 10]It is a figure showing the example of a format of validation key blocks.
[Drawing 11]It is a figure explaining the composition of the tag of validation key blocks.
[Drawing 12]It is a mimetic diagram of the managerial system of the contents which applied this invention.
[Drawing 13]It is a flow chart explaining contents incorporation processing of the client of drawing 1.
[Drawing 14]It is a figure showing the example of a format of contents.
[Drawing 15]It is a flow chart explaining the right-of-use generation processing of the client of drawing 1.
[Drawing 16]It is a figure showing the example of a format of the right of use.
[Drawing 17]It is a flow chart explaining contents playback processing of the client of drawing 1.
[Drawing 18]It is a flow chart explaining the details of the decoding processing in Step S46 of drawing 17.
[Drawing 19]It is the figure which expressed the decoding processing of drawing 18 typically.
[Drawing 20]It is a figure showing the example of the information included in EKB of drawing 19.
[Explanations of letters or numerals]
1-11-2 [A timer21CPUand 24 / An encryption decoding part25 codec partsand 26 / An input part27 outputting partsand 28 / A storage parts store and 29 / Communications department] A clientthe 2 Internetand 3 A content server and 4 A license server5 fee-collection serverand 20